# Office of Science & Technology Confidential Business Information (OST-CBI) Application Security Plan

**U.S. Environmental Protection Agency**
**Office of Water**
**Office of Science & Technology**

**June 10, 2003**

## SECTION 1.0 APPLICATION DESCRIPTION AND BACKGROUND INFORMATION

### 1.1 Application Description and Acronym

Office of Science and Technology (OST) Confidential Business Information (CBI)

### 1.2 Responsible Office

U.S. Environmental Protection Agency (EPA)
OST
1200 Pennsylvania Avenue
Washington, DC 20460

### 1.3 Category

Major Application

### 1.4 Points of Contact

*Security Plan Author and Application Security Manager (ASM)*

Name: Gregory Stapleton
Office: U.S. EPA, OST
1200 Pennsylvania Avenue, N.W.
Washington, DC 20460
Phone: (202)566-1028
E-Mail: stapleton.gregory@epa.gov

*Document Control Officer (DCO)*

Name: George Jett
Office: U.S. EPA, OST
1200 Pennsylvania Avenue, N.W.
Washington, DC 20460
Phone: (202)566-1070
E-Mail: jett.george@epa.gov

*RACF Security Administrator (RSA)*

Name: Jade Lee-Freeman
Office: U.S. EPA, OST
1200 Pennsylvania Avenue, N.W.
Washington, DC 20460
Phone: (202)566-1074
E-Mail: lee-freeman.jade@epa.gov

*Alternate RSA*

Name: Leonid Kopylev
Office: U.S. EPA, OST
1200 Pennsylvania Avenue, N.W.
Washington, DC 20460
Phone: (202)566-2237
E-Mail: kopylev.leonid@epa.gov

*OW/OST LAN Manager*

Name: Vera Williams-Bower
Office: U.S. EPA, OST
1200 Pennsylvania Avenue, N.W.
Washington, DC 20460
Phone: (202)566-0412
E-Mail: williams.vera@epa.gov

*Enterprise Server Security Manager (ESM)*
Name: John Gibson
Office: U.S. EPA, OEI/OTOP/NTSD
109 Alexander Drive, Building NCC
Research Triangle Park, NC 27711
Phone: (919) 541-0112
E-Mail: gibson.john@epa.gov

*Enterprise Server Coordinator*
Name: Lynn Conger
Office: U.S. EPA, OEI/OTOP/NTSD
109 Alexander Drive, Building NCC
Research Triangle Park, NC 27711
Phone: (919) 541-1481
E-Mail: conger.lynn@epa.gov

*SIRMO*
Name: Andrew Battin
Office: U.S. EPA, OST
1200 Pennsylvania Avenue, N.W.
Washington, DC 20460
Phone: (202) 564-0383
E-Mail: battin.andrew@epa.gov

*ISO*
Name: Terry Howard
Office: U.S. EPA, OST
1200 Pennsylvania Avenue, N.W.
Washington, DC 20460
Phone: (202) 564-0385
E-Mail: howard.terry@epa.gov

*Primary Organization Head*
Name: G. Tracy Mehan
Office: U.S. EPA, OW
1200 Pennsylvania Avenue, N.W.
Washington, DC 20460
Phone: (202) 564-5700

*Plan Reviewer*
Name: Debra Nicoll
Office: U.S. EPA, OST
1200 Pennsylvania Avenue, N.W.
Washington, DC 20460
Phone: (202) 566-1020
E-Mail: nicoll.debra@epa.gov

*Authorizing Official*
Name: Mary T. Smith
Office: U.S. EPA, OST
1200 Pennsylvania Avenue, N.W.
Washington, DC 20460
Phone: (202)566-1000
E-Mail: smith.maryt@epa.gov

## 1.5 Operational Status

Operation/Maintenance Phase.

## 1.6 Application Purpose

The OST-CBI application is the process that OST's Engineering and Analysis Division (EAD) uses for protecting confidential business information while handling and analyzing that information. *Confidential Business Information (CBI)* is any document received or generated by EPA or its contractors, where the information originator declares it to be confidential in accordance with 40 CFR Part 2 Subpart B. These documents may be paper or computer-based (e.g., compact disks, diskettes, computer files). OST may protect other information if releasing it could inadvertently disclose CBI; this information would be protected as equivalent to CBI.

EAD uses CBI to develop regulations under the Clean Water Act. EAD uses CBI (trade secrets, intellectual property, commercial, financial, and other information) to determine the effectiveness of wastewater treatment technologies. EAD also uses CBI to determine operational and economic impacts on the affected industries. Data managed under the OST-CBI application are critical to OST's mission.

## 1.7 Application Location and Architecture

The OST-CBI application has two components: 1) paper and removable media CBI, and 2) mainframe CBI. These components are described below.

**Paper and Removable Media CBI**: The *paper and removable media CBI* component refers to hard copies of OST-CBI and OST-CBI contained in computer files on removable media. CBI is not intentionally stored on computer hard drives; some software may automatically back-up data to prevent losing data during computer crashes. Examples of paper and computer documents that may contain CBI include the following:

- trip reports to industry facilities,
- questionnaires completed by facilities,
- code number lists used to mask CBI,
- electronic spreadsheets,
- MS Access databases,
- facility process diagrams, and
- cost information.

Paper and removable media CBI are located within EAD office space (i.e., individual offices, cubicles, and the CBI file room) within EPA headquarters at the following address:

EPA West Building
1301 Constitution Avenue, NW
6th Floor
Washington, D.C. 20004

EAD has protocols for accessing, handling, and tracking paper and removable media CBI - see *Security Plan for Confidential Business Information in the Engineering and Analysis Division* (April 10, 2000) which is included as Appendix A. That security plan (hereafter referred to as the *EAD Security Plan*) also delineates provisions for contractor use of CBI at their location.

**Mainframe CBI**: *Mainframe CBI* refers to the OST-CBI stored on the IBM mainframe system at EPA's National Computer Center (NCC) at Research Triangle Park (RTP), NC. Mainframe CBI includes engineering data and sampling data that can be directly linked to proprietary industrial processes. EPA staff access the mainframe from EPA headquarters. Contractors access the mainframe from their own office locations.

Most EPA and contractor staff authorized to access mainframe CBI use SAS/Connect, a Windows-based interface, to program custom SAS algorithms. In this case, the data and the application reside on the mainframe. Staff may also access mainframe data using secure terminal emulation software. Additionally, staff may also transfer data directly to removable media (e.g., a "zip" disk or a CD) to perform local analyses using common software (e.g., Access, Excel, etc.) and programming languages (e.g., SAS). RSAs may grant access to mainframe OST-CBI under their rules of behavior in Section 3 of this security plan.

### 1.8 General Support System Information

The OST-CBI application has two general support systems. The document control officer (DCO) applies prescribed protocols to track both paper and removable media CBI – the DCO could be considered as the "third general support system." PCs are required to view and manipulate removable media CBI. The IBM mainframe at NCC is the general support system for handling mainframe CBI. EPA users use the EPA local area network (LAN) to connect to the mainframe.

Contractors and sub-contractors may handle and access paper, removable media, and mainframe CBI if they satisfy the requirements presented in this security plan and the *EAD Security Plan*. The general support systems for the OST-CBI application components are described below.

**DCO - Tracks paper and removable media CBI:** The protocols controlling this component of the application are described in the *EAD Security Plan*. The DCO (an EAD employee) is subject to the same management controls (e.g., routine performance reviews) and background checks as other employees. Section 1.4 above provides the DCO's contact information; the following is the DCO's work location:

EPA West Building
1301 Constitution Avenue, NW
6th Floor
Washington, D.C. 20004

**PC Workstations – Required to access removable media CBI:** Employees do not need computers to read paper CBI. However, employees must use PCs to access data on removable media CBI. Most of these PCs use the Windows 2000 Professional operating system. OST is currently phasing-out PCs that use the Windows 98 operating system. Each PC has a "zip" drive, a CD-ROM drive, or both to allow media to be removed and secured when it's not being used.

PCs connected to OW's LAN may be used to access CBI on removable media. Formerly, OST and other OW offices operated their LANs independently. OST operated its LAN under the "old" LAN Security Plan. Since then, OST and the other OW offices migrated to "shared services" architecture to more efficiently align IT resources with OW's mission.

A comprehensive OW LAN security plan is anticipated to be completed September 2003. The OW LAN security plan will acknowledge that removable media CBI could be used on PCs connected to the LAN. The LAN security plan will prescribe protocols to prevent unauthorized access to the LAN and PCs connected to it. Although a formal security plan is not yet in place, several security measures are already in-use such as a firewall, an intrusion detection system dynamic IP addresses, and other measures.

Section 1.4 above provides the OW/OST LAN Manager's contact information.

**Enterprise Server – Required to access mainframe CBI:** EPA's Enterprise Server is the general support system for mainframe CBI. It supports large-scale data processing and provides a national data repository for Agency environmental and administrative systems. The user organization includes EPA program offices, regional offices and lab sites, as well as external business partners (i.e., states, universities, and public access requirements). There are hundreds of applications installed on the Enterprise Server.

The Enterprise Server is an IBM Generation 6 (G6) CMOS mainframe. The G6 is air-cooled and has an internal refrigeration unit to cool the Modular Cooling Unit (MCU). The MCU houses all processors in a single ceramic block. It has 10 application processors built into the system, of which only three are currently enabled. The processors in the G6 are based on a Complex Instruction Set Chip (CISC). Also, the MCU has two cryptographic coprocessors which have the highest certification for commercial security ever awarded by the U.S. Government, known as Federal Information Processing Standard (FIPS) 140-1. These coprocessors assist in encrypting data and support the Triple Data Encryption Standard (Triple DES) as well as other encryption standards.

The Enterprise Server system is located in EPA's NCC. The NCC resides in building NCC, a GSA owned facility located at 109 Alexander Drive, RTP, NC. The Office of Administration and Resources Management (OARM), Administrative Services Division (ASD) is responsible for NCC's physical security. ASD provides the guard force, badge reader system, and procedures required to operate the building in accordance with Federal policy and NCC requirements.

The *Enterprise Server Security Plan* describes measures to protect this general support system. Section 1.4 above provides contact information for the Enterprise Server security manager (ESSM contact information)

### 1.9 System Interconnection and Information Sharing

The *EAD Security Plan* describes how EPA employees and contractors may receive access to the OST-CBI application. Under special circumstances, other agencies may be granted access to the OST-CBI application. Employees from non-EPA agencies must receive written authorization from appropriate OW management before accessing the application. The authorization must address the conditions for their access. For example, they must follow the same rules of behavior as EPA employees and sign non-disclosure agreements.

Data from the OST-CBI application are not linked to other databases or shared through a computer network.

### 1.10 Applicable Laws, Regulations, and Standards

The laws, regulations, and standards that apply to the OST-CBI regulation and this security plan include the following:

- Federal Water Pollution Control Act (i.e., the Clean Water Act)
- 40 CFR Part 2 Subpart B, "Confidentiality of Business Information"
- Computer Security Act of 1987
- OMB Circular A-130, "Management of Federal Information Resources"
- NIST Special Publication 800-18, Guide for developing Security Plans for Information Technology Systems," December 1998

### 1.11 General Description of Sensitivity

The *EPA Information Security Manual (ISM 2195A1)* describes information sensitivity in terms of *confidentiality, integrity, and availability.* The manual also explains how to determine the sensitivity level of *low, medium, or high* for each term. Sensitivity of the OST-CBI application is summarized in the table below.

| Sensitivity Determination per EPA Directive 2195 | | | |
|---|---|---|---|
| **Information Categories** | **Confidentiality** | **Integrity** | **Availability** |
| Mainframe CBI | High | High | Medium |
| Paper and Removable Media CBI | High | High | Medium |

The inadvertent disclosure of data managed under the OST-CBI application could cause competitive harm to the business or industry providing the information. It could also embarrass EPA, thereby impairing its ability to obtain necessary information for the effluent guidelines program or other EPA programs. The confidentiality requirements for CBI are *high.*

Data integrity must be protected to ensure EAD develops effluent limitation guidelines based on complete and accurate information. Compromised data integrity can undermine the defensibility of proposed and final rulemakings. Data from the OST-CBI application typically become part of the administrative record for EPA rulemakings. The integrity requirements for official Agency records are *high.*

The OST-CBI application must be available to allow OST to perform analyses in a timely manner. Compromised availability could result in delays that would prevent meeting court-ordered deadlines for promulgating rules. Missing those deadlines can result in litigation. The availability requirements are *medium* for information that could result in litigation if it were not available.

### 1.12 Why is OST-CBI considered a "Major Application"?

The Office of Water identified OST-CBI as a major application using the definitions specified by OMB Circular A-130, "Management of Federal Information Resources." These definitions are provided below:

- " 'application' means the use of information resources (information and information technology) to satisfy a specific set of user requirements."

- " 'major application' means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate."

OST-CBI is an *application* because OST (specifically the EAD user) uses CBI (i.e., information) to perform supporting analyses for the effluent guidelines program (i.e., uses the information to satisfy a specific set of user requirements). Additionally, information technology (e.g., PCs, the Enterprise Server, and business processes) is used to manage and use the information. OST-CBI is a *major* application because of its high sensitivity as discussed in the previous section.

## SECTION 2.0 MANAGEMENT CONTROLS

### 2.1 Risk Assessment and Management

**Paper and removable media CBI** –The overall vulnerability of paper and removable CBI is considered to be *low*. EAD follows standard operating procedures as prescribed in the *EAD Security Plan.* Additionally, a DCO is assigned the responsibility for tracking paper and removable media CBI and training staff on the appropriate use and protection of CBI. Automated badge access to EAD spaces is limited only to staff that have had the appropriate training for protecting the OST-CBI application.

Vulnerability to hackers is non-existent for paper CBI because it cannot be accessed from a computer or computer network.

Hacker vulnerability for removable media CBI is expected to be low because it is only loaded onto PCs when needed.[1] When removable media CBI is not in use, it is removed from the PC and secured. At that point, the media is not accessible from a computer or a computer network. When the medium is loaded onto a computer, several security measures help protect the removable media along with the permanently-mounted media (e.g., the hard drive). These measures include using a firewall, an intrusion detection system, and dynamic IP addresses. Workstations are only permitted to have one LAN connection. Additionally, operational policies include prohibiting users from storing CBI on their workstation hard drives and LAN drives and require them to shut-down their workstations at the end of the work day.

**Mainframe CBI** - EPA contracted SRA International, Inc. to perform a risk assessment on the OST-CBI major application. This risk assessment only focused on the mainframe CBI component of the application; it did not address the paper and removable media CBI component. This risk assessment was performed from March through May 2001; SRA delivered the final report to EPA on August 8, 2001. The SRA assessment addressed various risks to the OST-CBI application.

The SRA assessment rated each identified risk as *high, medium,* or *low.* These ratings were defined as follows:

- High (H): Indicates an issue that requires immediate attention to resolve and mitigate the issue. These issues may indicate that a significant design or decision-making must be performed to initiate the effort. Involvement of multiple organizations or decision-makers may be required.

- Medium (M): Indicates a moderate level of risk and that attention is needed to mitigate or resolve the issue.

- Low (L): Indicates a minimal level of risk. Issues identified should be reviewed to determine if any resolution will increase the positive support for the success of the security program and there will be no adverse impact on EPA missions or services.

The findings were grouped with respect to management, operational, and technical controls. EPA staff reviewed the findings to determine their validity and to determine the appropriate action needed.

### 2.2 Review of Security Controls

The OST-CBI Risk Assessment identified 7 high-risk issues and 10 medium-risk issues. The identified risks and actions taken to mitigate them are summarized in Appendix C.[2] Consequently, only 2 high-risk and 5 medium-risk issues remain. We expect to resolve the remaining issues by Fall 2003; some of these resolutions are discussed briefly in Appendix C.

### 2.3 Rules of Behavior

Personnel with access to the OST-CBI application and its data have been trained how to protect it. Each individual has been given the rules that relate to their responsibilities. These rules of behavior reflect the actions we took to mitigate the risks identified in the risk assessment. They are attached in Appendix B.

[1] As prohibited by the EAD Security Plan, data on removable media CBI are ***not*** loaded onto permanently-mounted hard drives.

[2] For security reasons, we decided not to discuss the risk assessment details in the body of this plan.

## SECTION 3.0 OPERATIONAL CONTROLS

### 3.1 Personnel Security

EAD has established procedures for accessing both components of the OST-CBI application. These procedures are described in the *EAD Security Plan* and the *Rules of Behavior for the OST-CBI Application.*

#### 3.1.1 Background Checks

Federal employees are subjected to background investigation through Office of Personnel Management (OPM) upon being hired.

Contractor personnel may be subject to pre-employment screening and background checks by the contractor. However, current contracts used by EAD do not require background checks for their employees who handle CBI.

#### 3.1.2 Specialized Training

Potential users must receive certifications for the following training before they receive access to the OST-CBI application and its data:

- *Information Technology (IT) Security Awareness E-Learning Training Program.* OEI provides this training through the EPA intranet. Certification must be renewed annually.
- *CBI Security Training.* The document control officer (DCO) provides this training and also oversees biannual review and testing. Certification must be renewed biannually for EAD staff and annually for others. Certification requires signing a Confidentiality Agreement. See *EAD Security Plan*.

#### 3.1.3 Separation of Duties

EAD implemented procedural controls to help prevent unauthorized or unnecessary access to the OST-CBI application. These controls are reflected in the *EAD Security Plan* and the *Rules of Behavior for the OST-CBI Application.* For example, an RSA may not grant access to mainframe CBI unless the potential user's supervisor, or other appropriate person, agrees the employee needs access.

#### 3.1.4 Least Privilege

OST-CBI users only access relevant CBI documents to perform their jobs. The DCO and RSA's *Rules of Behavior* require them to keep appropriate records that adequately justify each user's access.

#### 3.1.5 User Accountability

For paper and removable media CBI, users are required to sign-out CBI as described in the *EAD Security Plan.* The DCO tracks documents that are signed-out by each user. Users are responsible for CBI in their possession. For mainframe CBI, each user is assigned a unique identifier. Enterprise server audit trails track each user's actions while accessing mainframe CBI. Therefore, all users are held accountable for their actions.

#### 3.1.6 Termination

There are two types of termination procedures: friendly and unfriendly. For friendly terminations,

- the employee's supervisor performs an exit interview,

- the employee's supervisor must notify the appropriate personnel to remove the employee's access to the OST-CBI application.
- the employee must return CBI, keys, and badges.

For unfriendly terminations, the following occurs:

- an effort is made to collect CBI, keys, and badges,
- if they are still onsite, the employee is escorted offsite,
- the employee's supervisor must notify the appropriate personnel to revoke all access to the OST-CBI application immediately.

## 3.2 Physical and Environmental Protections

### 3.2.1 Physical Protection

Paper and removable media CBI are located within EAD spaces on the 6th Floor of the EPA West Building within EAD spaces at EPA Headquarters. EAD staff stores paper and removable media CBI within locking cabinets. Additionally, an automated badge access system controls access to the locking doors for EAD spaces. *Only EPA employees cleared by the ASM or DCO receive automated badge access.* 24/7 badge access is granted only to EAD employees and certain cleared OWOW employees[3]. Other EPA employees have access during regular business hours. Contractors have no badge access.

Security guards control access to EPA Headquarters, including the EPA West Building. EPA employees require their employee badges or other acceptable photo identification to enter EPA headquarters without assistance. Non-employees must present acceptable photo identification and be signed-in at a guard-controlled entrance and escorted by an EPA employee. The security guards monitor the facility at all times.

Mainframe CBI resides on EPA's Enterprise Server located in EPA's NCC. The *Enterprise Server Security Plan* describes physical protection measures to protect this general support system.

### 3.2.2 Environmental Protection

EAD spaces are temperature controlled and a wet-pipe fire suppression system is installed. Environmental protection for the Enterprise Server is covered in section 3.2.2 of the *Enterprise Server Security Plan.*

## 3.3 Input/Output Controls

Input/output controls help protect OST-CBI data from being lost, stolen, or inappropriately disclosed.

[3] These employees, who have offices directly adjacent to EAD space, require access to allow them to walk to and from the pantry and restrooms.

### 3.3.1 Paper and Removable Media CBI

The *EAD Security Plan* delineates procedures for the following CBI activities:

- receipt
- labeling
- tracking
- storage
- generation
- transmission
- reproduction
- destruction

Staff that need help with the procedures are encouraged to contact the DCO or ASM. The OST-CBI *Rules of Behavior* lists their phone numbers. All staff cleared to access OST-CBI receive these rules.

### 3.3.2 Mainframe CBI

As described in section 3.3 of the *Enterprise Server Security Plan,* the ES has a comprehensive customer support service (i.e., "the Help Desk"). It provides technical assistance, problem diagnosis and solution, and tracking and consultation for all ES methods, procedures, and hardware. They may be contacted at (800) 334-2405.

Section 3.3 of the *Enterprise Server Security Plan* describes overall input and output controls that apply to mainframe CBI, including those that apply to printouts.

## 3.4 Continuation of Operations (COOP) Planning

Contingency plans help EAD to continue its operations if access to the OST-CBI application is disrupted. Currently, only an informal COOP exists for the OST-CBI application. EAD took an action to develop a formal COOP and complete it by December 31, 2003.[4]

### 3.4.1 Paper and Removable Media CBI

The *EAD Security Plan* describes practices that help prevent losing or misplacing CBI documents, including removable media. Once received, the DCO stores original CBI in the CBI file room. The DCO provides paper and removable media CBI only to staff that are certified to handle CBI. Additionally, the DCO logs the transfer of CBI to EAD staff. The DCO does not sign-out original CBI documents to non-EAD staff.

Currently, there is no formal plan to recover CBI that is destroyed by fire or other adverse situations.

### 3.4.2 Mainframe CBI

Although the OST-CBI application and its data are backed-up routinely, EAD does not currently subscribe to disaster recovery services to protect this application. After a casualty or disaster event, applications that subscribe to disaster recovery services will be restored before those that do not. EAD took an action to determine whether these services are necessary with respect to its mission.

[4] The ASM will notify the SIRMO if this deadline cannot be achieved.

Like all applications and data on the Enterprise Server, the OST-CBI application and its data could be recovered using backups if a casualty or disaster event occurred at NCC. The Agency's goal is to restore all Enterprise Server services within 30 days of a disaster using emergency procurement authority. However, it is important to note that specific applications and their data may be restored sooner depending on their priority with respect to the Agency's mission.

All backups are stored electronically in the offsite tape library. The following is the schedule for routine backups:

- Incremental backups for data sets created or changed during the day are made nightly – the 14 previous versions are retained.
- Full volume backups (i.e., backups of *all* Agency applications and their data) are made monthly and retained for 90 days (i.e., 3 previous versions are retained).
- Full volume backups are also made semi-annually and retained for one year (i.e., 2 previous versions are retained).

Personnel with pagers and cell phones are on call to respond to problems with backups and to monitor backup processes.

When disaster recovery resources are used, additional steps are taken to protect and expedite restoring the application including:

- The complete application data sets are backed-up nightly and retained for 7 days.
- Special software is used to "tag" the application data so it can be located more easily within full volume backups.
- Equipment could be purchased (or leased) and set-up to run the application at an alternate location.

Subscribers to disaster recovery services must allow time to develop recovery procedures and hardware infrastructure. These services are described in more detail in the *Enterprise Server Security Plan.*

### 3.5 Data Integrity Controls

The *EAD Security Plan* describes procedures to protect paper and removable media CBI from accidental or malicious alteration or destruction. For example, users are encouraged to use logged and tracked copies of CBI documents and files instead of the originals (*EAD Security Plan* Section 3.2).

The *Enterprise Server Security Plan* describes how data integrity is maintained on the Enterprise Server, which is where mainframe CBI is stored.

### 3.6 Documentation

Once approved, the OST-CBI Security Planning Package will be used to manage the OST-CBI application. It consists of the following:

- Section 1: Assignment of Responsibility
- Section 2: **This** security plan, including the Rules of Behavior
- Section 3: Periodic Security Control Reviews
- Section 4: Authorization to Process

Other directly relevant documentation includes:

- Security Plan for Confidential Business Information in the Engineering and Analysis Division dated April 10, 2000
- Final Risk Assessment of the Environmental Protection Agency's OST-CBI, August 8, 2001
- Confidentiality Agreements for OST-CBI users
- Certifications for OST-CBI users (CBI Training, Information Technology Security Awareness Training
- CBI Tracking Logs
- Standard Operating Procedure: Using Mainframe Accounts Managed by the Office of Science and Technology, April 20,2001
- Enterprise Server Security Plan
- EPA Information Security Manual (ISM 2195A1)
- Application RACF Security Administrator's Guide

The following documents are under development:

- OW LAN General Support System Security Plan
- OST-CBI Application – Continuation of Operations Plan (COOP) – anticipated completion: December 31, 2003

### 3.7 Security Awareness and Training

Before an individual may access the OST-CBI application, they must receive certification that they successfully completed the following:

- CBI Security Training
- Information Technology (IT) Security Awareness E-Learning Training Program

CBI Security Training is generally given by the DCO (or ASM) on a one-on-one, as-needed basis. Users that are EAD staff must take refresher training biannually while others must take it annually. The Office of Environmental Information (OEI) provides the IT Security Awareness E-Learning Program using a web page on EPA's intranet; refresher training must be taken annually.

Beginning in early 2003, EAD also plans to regularly schedule activities to promote security awareness for OST-CBI. For example, EAD already uses e-mail alerts to inform OST-CBI users if problems arise or are anticipated. These activities are included in the Rules of Behavior for the DCO, RSA, and ASM.

## SECTION 4.0 TECHNICAL CONTROLS

### 4.1 User Identification and Authentication

Before accessing mainframe CBI, all users must identify themselves using by their user-id and authenticate their identity by using their password. Resource Access Control Facility (RACF) software checks the user-id and password then grants (or denies) the user access depending on the access profile contained in the user's account. The RACF software controls access to all the Agency's data on the Enterprise Server.

On a daily basis, NCC staff uses Consul/RACF and nightly TSSMS reports to identify users that are using “trivial” passwords. If they identify one of these users, NCC staff notifies their respective RSA who then consuls them on how to create an appropriate password. Users also receive training[5] on how to create effective passwords. System Administrators do not have access to user passwords[6].

## 4.2 Authorization and Access Controls

The DCO’s and RSA’s Rules of Behavior were written to explicitly include conditions for granting and accounting for access. Their Rules of Behavior also include conditions for reviewing each user’s need to maintain access.

A potential user is granted access to the OST-CBI application if they possess the proper certifications (see section 3.7) and they need access to perform their duties. The potential user must request access from the DCO (for paper and removable media CBI) or RSA (for mainframe CBI) and provide adequate justification; the potential user’s immediate supervisor, or other appropriate person, must agree with the request before access is granted. The DCO and RSA maintain appropriate documentation that demonstrates access was properly granted.

The DCO or RSA periodically also consults with the user’s immediate supervisor, or other appropriate person (e.g., the EPA Project Officer if the user is a contractor), to determine whether the user still has a valid need to access the OST-CBI application. If the user resigns, is transferred, or is terminated, the user’s immediate supervisor is required to give adequate notice to the DCO and RSA so the DCO and RSA can remove the user’s access; this requirement is reflected in the immediate supervisor’s Rules of Behavior.

Software controls exist to control access to mainframe CBI including:

- *Limited entries for incorrect passwords*: User access is suspended when someone (including the user) enters the wrong password for a particular user-ID three times in a row. If this happens, the user must ask the RSA to restore access.
- *Timeout controls*: The system will automatically blank associated display screens after 20 minutes of inactivity. The user will be logged off after two hours of inactivity.

*Logon Scripts*: At this time, there is no known way to prevent using automated scripts with embedded passwords to logon to the Enterprise Server. OTOP Operational Directive 210.08 and the user’s Rules of Behavior prohibit these scripts.

*Access Control Lists.* The ASM maintains an access control list for the OST-CBI application.

Access privileges will be revoked for users that intentionally violate their respective Rules of Behavior.

### 4.3 Public Access

The public is not authorized to access the OST-CBI application. Section 2.1 describes measures taken to minimize unauthorized access to paper and removable media CBI. The *Enterprise Server Security Plan* describes measures that apply to mainframe CBI.

### 4.4 Audit Trail Mechanisms

The RACF software produces audit trails.

[5] *Information Technology (IT) Security Awareness E-Learning Training Program*

[6] One-way encryption is used to protect the user’s password. The password is encrypted when it is sent from the user to the mainframe’s RACF software. It is also encrypted within the user’s account profile. The user’s password is not transmitted from the Enterprise Server.

As described in the *Enterprise Server Security Plan*, the Operations Security Staff audits system and user activity according to NTSD Standard Operating Procedures to detect unauthorized transactions and transaction attempts. Audit trails record appropriate information that assists in intrusion detection.

## 5.0 Abbreviations

| | |
|---|---|
| ASM | Application Security Manager |
| CBI | Confidential Business Information |
| COOP | Continuation of Operations Plan |
| DCO | Document Control Officer |
| EAD | Engineering & Analysis Division |
| EPA | Environmental Protection Agency |
| ESM | Enterprise Security Manager |
| ISO | Information Security Officer |
| LAN | Local Area Network |
| NCC | National Computer Center |
| NTSD | National Technology Services Division |
| OEI | Office of Environmental Information |
| OST | Office of Science & Technology |
| OTOP | Office of Technology, Operations, and Planning |
| OWOW | Office of Wetlands, Oceans, and Watersheds |
| RACF | Resource Access Control Facility |
| RSA | RACF Security Administrator |
| RTP | Research Triangle Park |
| SIRMO | Senior Information Resources Management Officer |
| TSSMS | Time Sharing Services Management System |

## 6.0 References

- 40 CFR Part 2 Subpart B, "Confidentiality of Business Information"
- Application RACF Security Administrator's Guide
- Computer Security Act of 1987
- Enterprise Server Security Plan 1223/001A, May 14, 2002
- EPA Information Security Manual 2195A
- Federal Water Pollution Control Act (i.e., the Clean Water Act)
- Final Risk Assessment of the Environmental Protection Agency's OST-CBI, SRA International (Contract No. 68-W-99-038 Task Order No. 044), August 8, 2001
- NIST Special Publication 800-18, Guide for developing Security Plans for Information Technology Systems," December 1998
- OMB Circular A-130, "Management of Federal Information Resources"
- Security Plan for Confidential Business Information in the Engineering and Analysis Division, April 10, 2000

## 7.0 SIRMO Approval of the Security Plan

I have reviewed the OST-CBI Application Security Plan and find that it adequately describes the following:

- The purpose the application serves to the Agency's effluent limitations guidelines program.
- The sensitivity of the application and the data associated with it.
- The cost effective controls that have been implemented which are commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of data.

I approve the OST-CBI Application Security Plan.

I also understand that the Continuation of Operations Plan (COOP) for the OST-CBI Application is expected to be complete by December 31, 2003. If this deadline cannot be met, I understand the ASM will contact me.

____________________________________
Andrew Battin, SIRMO OW

## Appendix A

# SECURITY PLAN FOR CONFIDENTIAL BUSINESS INFORMATION IN THE ENGINEERING AND ANALYSIS DIVISION

U.S. Environmental Protection Agency
Office of Water
Office of Science and Technology

May, 1992
Amended April, 1994
Amended June, 1998
Amended January 28, 1999
Amended April 10, 2000

40 CFR Para. 2.211

## SAFEGUARDING OF BUSINESS INFORMATION; PENALTY FOR WRONGFUL DISCLOSURE

(a) No EPA officer or employee may disclose, or use for his or her private gain or advantage, any business information which came into his or her possession, or to which he or she gained access, by virtue of his or her official position or employment, except as authorized by this subpart.

(b) Each EPA officer or employee who has custody or possession of business information shall take appropriate measures to properly safeguard such information and to protect against its improper disclosure.

(c) Violation of paragraph (a) or (b) of this section shall constitute grounds for dismissal, suspension, fine, or other adverse personnel action. Willful violation of paragraph (a) of this section may result in criminal prosecution under 18 U.S.C. 1905 or other applicable statute.

TABLE OF CONTENTS

TOPICAL HIGHLIGHTS

| | | |
|---|---|---|
| 1.0 | INTRODUCTION | -OST responsibility<br>-CBI defined for this Plan<br>-"Document" defined |
| 2.0 | ACCESS | |
| 2.1 | AUTHORIZATION | -DCO authorizes most<br>-Div. Director authorizes those outside EAD<br>-Each cleared person has personal ID #<br>-List of access cleared individuals |
| 2.2 | RESPONSIBILITY | |
| 2.2.1 | Document Control Officer | -Overall responsibility<br>-Reviews contractor's CBI plan and operation<br>-Guidance and training |
| 2.2.2 | Division Director | -Approves applicants from outside EAD |
| 2.2.3 | Project Manager | -Determines which CBI reply goes to EAD or contractor<br>-Reports those no longer needing CBI clearance |
| 2.2.4 | OST Staff | -Assuming CBI responsibility<br>-Finding unattended CBI<br>-Reporting lost or stolen |
| 2.2.5 | Non-OST Staff | -Can't photocopy on own<br>-Can't send to contractors |
| 2.3 | ACCESS TO CBI BY CONTRACTORS | -Compatible security plans<br>-Complementary logging procedures |
| 3.0 | STORAGE AND HANDLING OF CBI | |
| 3.1 | STORAGE | -Two locking levels<br>-DCO accesses all cabinets |

| | | |
|---|---|---|
| 3.2 | LOGGING AND CONTROL OF DOCS. | -What is sent to the DCO<br>-ID #s for incoming docs.<br>-What and how items logged<br>-Color coded cover sheets<br>-Contents/entries to Log<br>-CBI not stored on hard disks<br>-Use of "locator variables" |
| 3.3 | WORKING FOLDERS | -Folder logged as one document but may contain many CBI drafts and temporary unlogged CBI |
| 3.4 | RELEASE OF DOCUMENTS | -All or part of a document<br>-Time constraint on part<br>-Time constraint on non-travel use outside EAD<br>-Use of Sign-Out Sheets to loan CBI between staff, after leaving DCO control<br>-Loaning "Working Folders" |
| 3.5 | SAFEGUARDING DURING USE | |
| 3.5.1 | In the Office | -Lock when away from office<br>-Turn over when non-CBI visitors walk in<br>-Use of "Working Folders"<br>-Staff control of draft correspondence |
| 3.5.2 | On the Telephone | -Ensure CBI clearance<br>-Conference calls<br>-Authorized facility contact |
| 3.5.3 | In Meetings | -Clearance of participants<br>-Distribution of CBI copies |
| 3.5.4 | Printing | -Cleared person must be present, e.g. at the WIC |
| 3.5.5 | At Home | -Double wrapped<br>-In locked house or car |
| 3.5.6 | Personal Transmittal | -Assure all are cleared |

| | | |
|---|---|---|
| 3.5.7 | Trans. by Common Carrier | -Keep in possession<br>-Do not read in public<br>-Not checked in luggage<br>-Lock in hotel safe or car |
| 3.6 | REPRODUCTION | -By the DCO and contractor<br>-For use in working folder |
| 3.7 | DESTRUCTION | -Shredding paper and over-writing disks<br>-Special software to over-write hard drive files |
| 3.8 | USE IN NON-CBI DOCUMENTS | -Avoid identifying facility in study findings |
| 3.9 | INTERNAL AUDITS | -Audits/reporting violations |
| 4.0 | <u>TRANSMITTAL OF CBI</u> | -Double wrapped and labeled<br>-Follow-up on shipments |

GLOSSARY

# LIST OF FIGURES

# 1.0 INTRODUCTION

While developing effluent limitation guidelines and standards, the Engineering and Analysis Division (EAD), Office of Science and Technology (OST) will collect, handle and store confidential business information (CBI). Under the provisions of 40 CFR Part 2 Subpart B, OST is obligated to protect CBI from unauthorized disclosure.

This Security Plan establishes the required procedures that EAD staff must use to safeguard CBI, which is collected or generated for EAD's rulemaking. Staff from other EPA offices, who use this CBI, are also required to comply with the Plan. A separate Implementation Plan for EAD staff addresses how this Security Plan is incorporated into the ongoing work of the Division. Contractor staff who use this CBI are required to have an EAD-approved security plan that is compatible with the EAD Plan.

"Confidential Business Information" (CBI) is defined as any disk or document received or generated by EPA or by an EPA contractor, where the originator of data or information declares it to be confidential, in accordance with 40 CFR Part 2 Subpart B. At the time of submission, a business may assert a business confidentiality claim by "placing on (or attaching to) the information...a cover sheet, stamped or typed legend, or other...notice employing language such as trade secret, proprietary, or company confidential." Such designations may also be made on inside pages or verbally by the facility. EAD policy is to accept any such declarations as valid. These designations may be modified as the result of subsequent EAD inquiries and determinations by the Office of General Counsel. CBI material also includes any EAD-generated disks, documents, or PCs on which CBI is produced or stored and which incorporate submitted CBI information. For convenience, the term "facility" will be used hereafter in the Plan, when referring to <u>all sources</u> of CBI submission from outside of EAD.

Any questionnaire, letter, memorandum, analytical data, technical or other report is considered to be a "document." That document may be in paper form or a file in a computer disk. Therefore, whenever the term "document" appears in this Plan, it is under-stood to include paper copy <u>and</u> diskettes -but not individual files on diskettes. Separately bound attachments may be handled as separate documents. If separated, a list of those attachments will be produced and accompany the original document.

# 2.0 ACCESS

## 2.1 AUTHORIZATION

Only the EAD Document Control Officer (DCO) or the Alternate Document Control Officer (ADCO) can release EAD CBI material.

Only authorized EPA employees or those of its contractors, approved for access to certain CBI material, will be allowed access to EAD CBI. This access is available by two means, depending on whether EAD or other EPA staff are requesting it.

1. EAD staff may gain access by completing all of the following: (1) reading the provisions of 40 CFR Part 2; (2) reading this Security Plan; (3) passing a brief written test on the Plan from the DCO; and (4) signing the Confidentiality Agreement, which acknowledges that they have read and understand the Plan and agree to abide by it. Figure 1 shows the Agreement and Figure 2 shows relevant portions of 40 CFR Part 2. Copies of the Agreement are available from the DCO, who also provides guidance and advice regarding use of the Plan. Staff will be required to take a written test every two years as a refresher (rev. 12/11/96).

2. EPA staff outside of EAD must, additionally, submit a written request, through the Project Manager, to the EAD Director, justifying a need for access. That memorandum (Example shown in Figure 3) must also state that the access requested is a limited privilege and will not continue beyond the period of legitimate need. In any case, this authorization will not exceed one year. Such authorization may be renewed, subject to approval by the Project Manager. The requester specifically acknowledges that notification must be given to the Director and the DCO upon early completion of the requester's need. The requester also acknowledges that he/she will provide the necessary physical security for any CBI released to them. On rare occasions, and with the concurrence of the Division Director, verbal requests for access may be accepted in place of this written justification. In such case, the Project Manager will be notified of this fact.

3. If a non-EAD applicant has been approved under another program's CBI security plan and that plan is at least as stringent as our own, that individual need not take our exam to be cleared for access to EAD CBI. The DCO makes this determination. However, he/she will be given copies of the complete and abbreviated plan and asked to acknowledge in writing that these have been read, understood and will be complied with (Figure 9).

Approved EPA staff may be issued identification numbers by the DCO, to facilitate accountability of CBI material.

The signed Agreements are retained by the DCO, who maintains a list of EPA personnel authorized for CBI access to specific projects and distributes a current list to OST and contractor staff with a need to know.

When CBI in the effluent guidelines computer databases are requested from EAD staff, the DCO must first be contacted to verify that the requester is CBI cleared. Only the personnel specified will have access to that particular database or database subset.

The named representative of a facility, who originally supplied CBI to the Division does not require special clearance and is considered to be cleared for discussion or correspondence on what the facility provided.

The DCO may, at his discretion, deny the release of all or part of any request, pending additional clearance by the DCO's supervisor. Such circumstances may include (but are not limited to) apparent incapacity of the requester or the unusual nature of a request, such as for all the CBI files of the Division, etc. The DCO may also initiate action to cancel anyone's clearance, subject to review and approval by the Director.

## 2.2 RESPONSIBILITY

### 2.2.1 Document Control Officer

The Document Control Officer is responsible for implementing and maintaining the Confidential Business Information (CBI) Security Plan of the Engineering and Analysis Division and for maintaining security of all documents under his control. The Alternate Document Control Officer (ADCO) exercises all the functions of the DCO in his absence, or as requested by the DCO. Only the DCO or ADCO may release CBI material from the "Central CBI File." This File is the physical repository of all CBI documents, which are logged into EAD, and which are not otherwise signed out to other staff. The DCO maintains current record keeping in a readily accessible, current and thorough manner.

The DCO visits or arranges for inspections of EAD contractor facilities to review operational management of their CBI plans. He reports findings and recommendations to the EAD contract Project Officer.

Through individual guidance or training, the DCO ensures that EPA staff, requesting CBI clearance, read and understand the Plan and sign the Confidentiality Agreement. He informs EPA staff, who have a need to know, on how to secure access-clearance and how to request, safeguard, use and transmit CBI information.

He works with Division supervisors regarding the inclusion in Performance Agreements, as appropriate, of Standards or elements of Standards which acknowledge CBI responsibility. He provides guidance and instruction to the Alternate Document Control Officer in the exercise of his/her duties.

If any substantive question arises regarding interpretation of some part of this Plan or some security contingency not covered by it, the DCO will make that decision and document this circumstance as an addendum to the Plan. Parties may appeal such decisions to the EAD Deputy Director or Director. As necessary, the DCO will submit written revisions to this Plan for approval by the EAD Director, after review and comment by the Branch Chiefs.

The DCO is not responsible for the security violations of others who are cleared for access to EAD's CBI, whenever CBI material has been properly transferred to them and is no longer under the DCO's immediate physical control.

### 2.2.2 Division Director

The EAD Director is responsible for notifying the DCO when an EPA employee from outside the Division is approved for clearance processing according to this Plan. He must also forward to the DCO any notice received that outside-Division staff no longer need CBI clearance.

### 2.2.3 Project Manager

The Project Managers for each rule/project shall determine if specific documents, such as responses to questionnaires, will be mailed directly to EPA or to contractor offices. For CBI addressed to EAD, Division staff are required to ask contractors, facilities and others to mail this to the DCO as the initial delivery point. However, draft CBI correspondence received for 1-2 day review and return -but not for permanent retention by EAD- may be mailed directly to EAD staff and will not be logged by the DCO. EAD recommends that large survey responses be sent directly to contractors, unless initial review of the material needs to be done by EPA (Documents should not be mailed to EPA, only to be repackaged and then mailed to contractors).

It is also important for Project Managers in early correspondence with facilities to request the names and phone numbers of cleared contacts for discussing CBI, along with their supervisors. The latter are needed, in case the previously designated contact is replaced by someone new, and EAD wants to verify this.

When the Project Manager determines that an EAD (or EPA) employee no longer requires CBI access, then the DCO must be notified so that the employee's name can be removed from the authorized list.

### 2.2.4 OST Staff

CBI documents signed out to a cleared EPA staff member are the responsibility of that person, while under their immediate physical control. However, when released to or accessed by others through approved procedures, that responsibility transfers to the recipient. When the user no longer needs that material, he/she must return it to the previous owner. If this was the DCO, he will promptly return it to the Central File and note this in the log.

Anyone finding a CBI document unattended shall return it to the DCO. The finder should, additionally, leave a note for the absent individual, indicating the action taken.

Those who are charged with responsibility for specific CBI documents must orally report any lost or stolen CBI to their supervisor and the DCO, as soon as it is known, including any facts surrounding the event. The reporting individual must also submit a signed, written report within three days of the oral report, detailing circumstances surrounding the loss, through his or her supervisor to the DCO.

### 2.2.5 Non-OST EPA Staff

In addition to following other aspects of this Plan, EPA staff from outside of EAD are specifically enjoined not to make photo-copies of any CBI documents they receive from EAD. Additional copies may be obtained through their own DCO or -if none assigned- directly from the EAD DCO. For effective document management, it is preferable that DCO's make such arrangements with each other on behalf of third parties. Also, non-OST EPA staff may not send CBI, derived from EAD, to any contractor or other recipient outside of EPA. If this is necessary, they must return such material to the DCO, who will clear this request with the Project Manager and arrange proper transmission, after verification that the recipient is CBI cleared.

## 2.3 ACCESS TO CBI BY CONTRACTORS

EPA staff may disclose CBI to authorized contractors or subcontractors performing work for EPA. The clauses addressing this, as required under 40 CFR Part 2, are incorporated into existing contracts. EPA is also required to notify the affected facilities by letter or by a Federal Register notice if any contractors will receive CBI.

Contractors and subcontractors that perform guidelines work on behalf of this Division have authorized clearance to CBI, if they have security plans approved by the appropriate contract Project Officers, in consultation with the DCO. Current and new plans must be compatible with the EAD CBI Security Plan to expedite document transfer between OST and contractors and to maintain an accountability bridge. All contractors supporting EAD CBI work will acknowledge in writing that they have read and understand the provisions of 40 CFR Part 2, the procedures of this CBI Security Plan, and the necessity of adopting a compatible CBI plan of their own.

The following elements are recommended in the contractor's plan to promote compatibility with this Plan:

(a) A written CBI security plan that clearly defines responsibilities and procedures.

(b) A counterpart DCO appointed to manage and ensure compliance with the contractor's plan.

(c) Continuous physical security of CBI documents to prevent access by non-CBI cleared individuals.

(d) Users will not store CBI on the hard disk of a personal computer or in a “permanent archive” of the Mainframe, since the latter is not under the complete control of the user.

(e) Assignment of a unique, document identification (ID) number to each permanent (non-"Working Folder") document.

(f) A log that identifies and locates all CBI documents contained in secured files along with the corresponding document identification numbers.

(g) Secure transmission of CBI documents by contractor staff, through third party or commercial carriers, when sent outside the contractor's offices.

(1) To the extent possible and consistent with timeliness, but without extensive reworking of original material, sections of CBI should be excluded if not required by the addressee (rev. 1/28/99).

(2) All CBI for EPA employees should be sent through the Engineering and Analysis Division Document Control Officer (EAD DCO) (rev. 1/28/99).

(3) Written monthly reports on the status of all transmittals from the contractor site to any other location should be sent to the EAD DCO (rev. 1/28/99).

(h) Acknowledgment that only the EAD DCO may destroy or authorize destruction of original CBI documents that were obtained from facilities and initially received by EAD. Also, he shall be notified within two weeks, in writing, of any EAD-logged CBI material that is destroyed or -in the case of disks-erased. Notifica- tion must include the document ID numbers and should additionally include document titles or summary disk titles -but not individual titles or entries on each disk. None of this refers to CBI originally received by or generated by a contractor.

(i) Destruction of CBI by document shredding, overwriting or destruction of disks, and electronic removal from mainframe computers to preclude any recall of that information.

(j) Acknowledgment that, at the end of a contract, all remaining CBI material generated or received as a result of this contract and still possessed, is the property of EPA and will be returned to it. This will include a complete inventory and accounting of all CBI handled during the contract period.

(k) No storage of CBI on any computer’s hard disk or on a “permanent archive” in the

Mainframe, since the latter is not under the complete control of the user.

## 3.0 STORAGE AND HANDLING OF CBI

### 3.1 STORAGE

All CBI, including documents and CBI records on hard disk drives, shall be stored with at least two levels of locks. When CBI is stored on the hard drive of a Macintosh PC, the password and an encryption file will suffice as one of the two locking levels. Otherwise, the Macintosh or IBM PC requires a physical lock on the hard drive. At the end of each working day, all CBI documents, except those in the possession of traveling employees or on temporary home loan, will be returned to appropriate storage areas.

The DCO maintains information on the location and type of all CBI locking cabinets, files or other containers and maintains keys and combinations to each. Only three keys or knowledge-of-combinations should exist at any given time for each of the two locking levels: (1) one with a locking-file-cabinet owner,
(2) one with the DCO, and (3) one optional key for allocation -or retention- by the branch chief.

### 3.2 LOGGING AND CONTROL OF DOCUMENTS

All documents received at EAD via registered mail or Federal Express that are not addressed to a Division employee will be first given to the DCO. All other CBI, will be promptly sent to the DCO for log-in, after opening and review by the addressee.

Each document received by any employee shall be examined to see if it contains confidential business information. If any part of a bound document contains CBI, the entire document is handled as CBI. All new CBI designated documents received from outside sources are given to the DCO for entry into the Division's document tracking system. A Project Manager may also decide if a non-CBI document should be handled according to CBI procedures, such as a questionnaire. If so, it is logged as non-CBI but is handled thereafter as if it were CBI.

Final (not draft) CBI documents created by EAD must also be given to the DCO for logging. Correspondence with contractors or facilities, that does not contain CBI information is not logged.

Draft CBI documents received from a contractor or other non-EAD source for 1-2 day turnaround/review, which are not intended for retention, are not logged by the DCO. They are retained in the Working Folder. Responsibility for their control rests with the originator.

The DCO assigns a unique identification (ID) number to each incoming CBI document or disk, with part of the number sequence being unique to that project. A set of disks that is maintained together may receive one ID #, but each disk will receive an individual sub-set number (e.g. "00016.1" or "00016.2" for disk 0.1 in set 00016, etc.). The DCO records this information electronically in the Master CBI Log. As such documents leave the Central CBI File or are eliminated, the DCO modifies Log entries accordingly. Such documents may be removed from the Central File through sign-out for EAD work, transmission outside of EAD, planned destruction, or information retrieval from a disk.

The DCO will attach to each document a Cover Sheet (Figure 4), with a color unique to a particular project or branch, providing entry blocks for the document ID number, name and signature of the DCO and document recipient, the recipient's office, and the date out and in. This attached Cover Sheet acknowledges transfer of responsibility for that material and must not be removed.

The first and last page of each paper document will be stamped "CONFIDENTIAL BUSINESS INFORMATION," and the last page will be stamped "LAST PAGE, Document ID# ____." This is to bring to quick attention the loss of any end pages which become detached, such as from thick, stapled documents. The DCO will mark the edge of documents more than one inch thick with a diagonal slash.

It is recommended that EPA staff ask for copies of documents rather than originals, to allow for adding notations, edits or similar modifications. Photocopies of a document will be identified in the Master Log by the ID number of the original, plus an added numerical identifier, indicating which numbered copy it is (e.g. "00012.4" for copy 4 of "00012"). This modified CBI number will be placed on both the Cover Sheet and the first page of each document (or on the disk).

Colored disks will be issued for CBI-only use. Colored Cover Sheets and/or labels will be unique to certain projects or branches. Examples of CBI that might be generated and stored on diskette are: text files with CBI; spread sheets, databases and diagrams; and CBI copies from another computer file.

CBI or other controlled access documents received from other offices within EPA or from other federal agencies shall be routinely logged into and controlled under EAD's CBI system.

Material classified as CBI but subsequently found to be non-CBI will be purged from the tracking system (Except non-CBI documents requested for CBI handling by a Project Manager; Para. 2 of 3.2). The DCO logs CBI that is incoming, loaned and transmitted outside of EAD. The computer Master CBI Log for the Central CBI File will include information on each item's current ID number (and any previous number, if assigned), whether it is CBI or non-CBI, draft or final, title, date received, whether an original or copy, and name of the receiver. This information will also include four additional subset information fields for that material:

(1) For Survey responses to questionnaires - the name and address of the facility and the Survey ID number;

(2) For transmittals within EAD - to whom, the date and a brief description section on

what was transmitted -e.g. the complete document, a part (e.g. pgs.XX-XXX) or a copy;

(3) For tracking of CBI material sent to or received from outside of EAD through certified return-receipt mail, commercial carriers, couriers, etc. Transmittals outside of EAD will include fields on the due date, when received, by whom, and the condition received.

(4) Date of physical destruction or electronic information removal, whether all or part was involved, if part -what that was, and the witness thereto.

Summary information may be selectively or comprehensively called up from the Master CBI Log by date/entry fields either for documents (1) logged in, (2) transmitted within EAD from the Central File, (3) transmitted from the Central File to outside of EAD, (4) destroyed or cleared of CBI content, and for lists of documents by (5) names of individuals who have signed them out.

The DCO backs-up the computer log file at least daily and maintains a daily transaction printout of the previous day's log actions, in case of computer or power failure.

Users will <u>not</u> store CBI on the hard disk of a personal computer. Any on-site storage will be onto a ZIP-drive, floppy or CD ROM disk. These diskettes will be safe-guarded as if they were CBI documents and stored under double locks at the end of the workday. If unusual circumstances temporarily require that CBI be stored on a hard disk drive, the entire PC will be handled as if it was CBI and kept under double locks. One of these may be the key lock to the main unit of the PC. The CBI files will also be considered "locked" if a password is used with encryption of the files (e.g. the Norton utility Diskreet, which encrypts a file, that can only then be used with a password).

CBI stored in mainframe computers will be protected under the Resource Access Control Facility (RCAF) to allow access only to authorized EPA staff and contractors. To the extent possible, only CBI <u>without</u> "locator variables" should be placed on the mainframe computer at EPA's National Computer Center (NCC). "Locator variables" are facility name, address, and any information which could identify a facility if used in conjunction with publicly available information (for example, the NPDES number). Facility ID numbers which have been randomly generated to identify data for the facilities are not considered locator variables. Locator variables can be placed on a CBI diskette or hard copy for reference.

## 3.3 WORKING FOLDERS

A "Working Folder" will be maintained as a CBI document and may be either a diskette or an actual folder. If a Folder, each paper or document cover inside must be stamped as "CBI" -but will not otherwise be logged or identified by the DCO. CBI stamps will be issued to Project Managers by the DCO for distribution to their staffs. Examples of these contents might include written comments, phoned inquiries and responses, notes for a memo or letter, draft reports, printouts from a file containing CBI, and tables. It is recommended that the number of such Folders be kept to a minimum. "Working Folders" will be colored or color labelled in a way that is unique to a particular project or branch. Folders should not become so bulky that they are awkward to use or store. In this case, the responsible staff person should weed out old material and give it to the DCO for destruction or, if necessary, create a new Working Folder.

## 3.4 RELEASE OF DOCUMENTS

The DCO may log out all or part of a project document to a CBI cleared EAD staff person, working on that project, or to others with the Project Manager's approval. If part of a document is requested, it may not be removed from the Central CBI File for more than 24 hours. Whole documents may be signed out to EAD staff for as long as required by the project mission. If only part of a document is requested, the DCO inserts a computer generated "Marker" sheet in the original document, where that part was taken. This identifies the missing contents by page numbers or description, the person to which assigned, their initial(s), and date of removal. After leaving the DCO, parts of documents may not later be separated into smaller parts for loan between staff members. Each part will be treated as a separate CBI document and receive both an identification number and a Cover Sheet.

Circulation of original CBI documents received by EAD may not go beyond EAD staff.

The DCO may log out excerpts and full documents (non-travel requirements) for overnight or weekend use -or as otherwise authorized by the DCO. Such requests should only be granted on an exceptional need basis.

An EAD staff person may loan CBI documents to another EAD staff person for up to a calendar week, if this information is noted on a visibly displayed CBI Sign-Out Sheet (Figure 5) in the user's office, identifying the current user ("Owner"), date in or out, ID number of material loaned, and the borrower's name. This formally acknowledges transfer of responsibility for each document. When a CBI document is no longer needed, it must be returned to the previous owner. These Sign-Out Sheets shall be turned in to the DCO, when they are filled up or no longer needed. Mistaken entries shall only be lined through with one or two lines but not obliterated so they are unreadable.

The CBI stamped contents of a "Working Folder" may also be loaned to another employee. These documents will be subject to the same control procedures as other CBI, except that they are not logged and controlled by the DCO and a Cover Sheet is not attached. Remember, that -as with other CBI transmittals within EAD, they must be hand delivered and received by the recipient or by a CBI cleared staff person with locking files (not left in an In-Box or on a chair).

Loaned parts of Working Folders should be placed in colored file folders or with colored labels for specific projects and/or branches.

When an employee is absent and another EAD employee who is working on that project needs CBI material that was signed out to the absent employee, only the DCO or ADCO may transfer that material. Either must accompany the requester, to the absent employee's office and ensure that the transfer is properly recorded.

## 3.5 SAFEGUARDS DURING USE

### 3.5.1 In the Office

When a non-EAD person enters a work area, where work with CBI is being performed, the person responsible for the CBI must cover the material, file it, or place it face down. If the employee in possession of CBI must leave the workplace for a short period, the material must be placed under the first level of lock, as in a locked drawer, file or individual locked office, or returned to the CBI Central File. If using CBI on a PC and the operator must temporarily leave the PC, the door must be locked or the computer session terminated. CBI material must be personally conveyed from office to office and personally received by CBI cleared staff. Such material will not be sent via route slips, in standard envelops, or under similar cover between offices.

It will not be left on top of furniture or the floor for absent employees. Otherwise -and at the end of the day, CBI must be kept in locked files or in a PC that is secured, such as by a password with an encryption file or keylock, when not in use, and behind a second level of locks (e.g. a locked door).

Draft correspondence containing Division generated CBI text is the responsibility of the EAD staff person who creates it. It may be retained as part of the Working Folder and stamped "CBI" or it can be given to the DCO for logging, control and a Cover Sheet. If it is kept in the Working Folder, it may be loaned to other EAD staff -but should be placed in a project-specific colored file folder, while in transit.

If a CBI attachment, which was previously logged and numbered by the DCO, is added to the draft document, the two must be transmitted under separate covers as they move between staff for review and changes. When finalized and signed, the draft document must be given to the DCO for logging.

### 3.5.2 On the Telephone

As much as possible, EAD staff should avoid discussing CBI over the telephone, due to the difficulty of assuring secure communication. If this is unavoidable, EAD staff must make a reasonable effort to determine that individuals they are speaking with are cleared for CBI, that those individuals are speaking on a private line (not shared with others), and that they are not using a speaker phone or voice box (unless approved for a meeting). EAD staff must also indicate at what point CBI will be discussed. As an added precaution against unanticipated listeners, they must (1) always refer to a facility by its ID number and never by its name and (2) speak circumspectly about specific items of information, such that only a listener would understand who shares the same information. For example: "I have a question about the sample taken next to the depot;" "When did you acquire your data on page 16, paragraph 4?;" or "Which process did you use at Mill Number 12?"

Conference calls or speaker phone connections must not be arranged, where others may dial in and listen (possible with EPA arranged BRIDGE teleconferencing or with a hotel switchboard).

Any telephone conversation with a facility representative on CBI issues that involves an understanding with an EPA employee must be documented in written notes. Such documentation will be filed in the Working Folder. Any substantive understandings reached over the phone must be followed by a confirming memorandum between the callers, based on these notes. If it contains CBI, that memorandum will be logged by the DCO. All telephone conversations involving CBI should be documented in writing.

If an EPA or contractor employee must contact (phone or write) a facility to discuss CBI provided by it, they must call the named facility contact previously identified by it for that information. It is desirable for the facility to authorize two contacts for such discussions. If not previously done through initial correspondence with the facility, initial phone calls should also identify the facility contact's immediate supervisor. This will allow verification of a replacement contact, if the original one becomes unavailable or absent. EPA and contractor employees must not speak with any other facility personnel without permission of the listed facility contact or his/her supervisor. Conversations with facility attorneys must be conducted carefully to avoid making careless statements that could prejudice the mission of the Division, OST or OW.

If a facility or person contacts EPA about specific project CBI, the recipient of the call will verify that the caller is on the list of approved names for that project. If there is doubt, the EAD employee will tell the caller that he/she will call back, after which the caller's identity or correct private phone number can be verified.

### 3.5.3 In Meetings

Copies required for distribution must be given identifying numbers by the DCO and logged out to the Project Manager before the meeting begins. Before discussing or distributing CBI material, the Project Manager is responsible for assuring that all attendees are cleared. The DCO will provide a list of cleared EPA participants (who have signed the Confidentiality Agreement). If the meeting includes contractor staff, the contractor's DCO will inform the Project Manager about cleared contractor staff. If a facility is involved, the facility contact shall do the same for any participating facility staff.

The Project Manager is also responsible for recovering all copies of CBI material, at the end of the meeting. When copies are distributed for retention by participants, the Project Manager will bring one or more Sign-Out sheets and ensure that documents are properly signed over to CBI cleared recipients. At the start of the meeting, he will announce that CBI will be discussed. If any meeting member is not so cleared, that person must leave or the meeting cannot continue. He/she will also remind participants of their responsibility for safeguarding CBI, especially meeting notes. After the meeting, the Project Manager will ensure that nothing is left in the room, such as written notes on the table, in waste cans or on a blackboard. The Project Manager retains the sign out sheet(s) to ensure return of all documents.

When possible, EAD recommends mailing or delivering documents containing CBI to meeting participants before the date of the meeting. EAD does not recommend the use of CBI at large work group meetings.

### 3.5.4 Printing

CBI should be printed in a secure EAD or contractor office. If it must be printed elsewhere, such as the EPA WIC, a CBI cleared EAD or approved contractor staff person must be present to receive the document as it is printed.

### 3.5.5 At Home

OST employees are discouraged from taking CBI home, however this may be done with notification to the DCO. When not in use, such material shall be locked in a house or a car and double wrapped/ labelled as it would normally be in transit outside the Division (See 4.0, Transmittal of CBI). CBI material from a contractor may be delivered to an EPA employee at home without prior notification to the DCO. In this instance, it is considered to be under the contractor's control system, until it is brought to EAD and logged in by the DCO.

### 3.5.6 Personal Transmittal

Before an EAD or contractor staff person conveys CBI material to someone outside of EAD, the DCO will ensure that both are on the approved list for CBI clearance and will notify the Project Manager before that material leaves EAD.

### 3.5.7 Travel by Commercial Carrier

EAD employees should avoid traveling with CBI. If it is necessary to carry this material to perform duties, the employee must tell the DCO which CBI material is being taken, before leaving. Named contacts in individual facilities that submitted CBI may receive their own CBI or subsequently created documents that are derived from it.

Employees shall keep any such material in their possession at all times and double wrap and seal it, when not in use. Travelers should be sure to carry or secure local access to whatever tape or stapler is necessary to re-seal such material. CBI documents shall not be checked in luggage, when using a commercial carrier. CBI shall not be read while in unrestricted access public facilities, such as in public transportation waiting rooms or in a plane or train. CBI materials must not be left unattended in a hotel room and, when not in use, must be stored in hotel or motel safes, in a room safe if provided, or inside the locked portion of a motor vehicle. A locked briefcase is not considered secure without additional protection, as mentioned above. Receipts will be obtained, if CBI is stored in a hotel or motel safe. At the end of the trip, a traveler may temporarily take CBI material home, if it is inconvenient to return directly to EAD.

## 3.6 REPRODUCTION

Portions of CBI documents may be photocopied by EAD staff and placed in Working Folders. However, if the copy is for another purpose other than for a working folder, the DCO -or someone acting under his supervision- must make the copy and assign an identification number. In the event of a heavy photocopying workload, the DCO may request temporary assistance from the chief of the branch, which requested this service. Non-EAD staff may not photocopy any portion of a CBI document.

Unusable CBI copies that result from copy machine jams or malfunctions must be returned to the DCO for destruction. Be sure that all copied pages have been removed from the machine before leaving it.

Documents may be reproduced only by the DCO or by contractors authorized to support the CBI work of the Division (See next paragraph for exception to this). All photo-copies, as well as disk copies, must be logged and controlled as separate documents, when they are created. Also stamped on the cover page of each copy will be the warning "DO NOT REPRODUCE," which is a reminder that no one other than the DCO can make copies of complete documents.
No EAD staff person who receives a copy (or original) is authorized to further reproduce any part of that document, unless that part is for use in a Working Folder. Otherwise, additional copies must be requested from the DCO.

As necessary for sharing information with non-CBI cleared recipients, or to limit additional logging/control requirements of others, CBI sections may be removed, blocked out or covered and the balance of that document reproduced by any EAD staff person for such use. Portions of original CBI copies that are blocked out with ink or similar substance will continue to be safeguarded as CBI or returned to the DCO for destruction to ensure against image recovery by others from the marked-over area.

## 3.7 DESTRUCTION

Only the DCO may destroy or authorize destruction of CBI documents that were created by EAD or were received by it from facilities. CBI hard copies and all or parts of Working Folders no longer needed by EAD staff must be returned to the DCO for destruction by shredding. He will secure permission from the Project Manager before any original material is destroyed and will maintain custody of all CBI documents until this is done. CBI document copies sent to a contractor may be disposed of under the contractor's CBI plan, unless EAD requests their return. However, the contractor's DCO should provide the EAD DCO with a memorandum that identifies the destroyed material by log number and title. Document segments will be identified by page numbers or by complete chapters, appendices, etc., when complete sections are involved. When material is destroyed, the DCO records this on the Destruction Log (Figure 8) and in the Master Log. Document ID Numbers will not be assigned to contents of Working Folders for destruction purposes.

When CBI stored on magnetic media are no longer needed, the DCO must personally ensure that it is either destroyed by cutting disks in half or by electronically clearing diskettes, so that contents are permanently removed. Diskettes can be electronically cleared by (1) overwriting, using special software, such as the Norton Wipeinfo command (with the Government Wipe option) or (2) by reformatting the diskette, using an option which will not allow files to be recovered (such as the unconditional format option in DOS 5.0). Simply "erasing" files is insufficient, because those same files can be unerased and recovered.

Removing CBI files on the hard drive of a PC is the responsibility of the originator of those files. In such cases, the DOS commands Erase and Delete should not be used, because data are still recoverable. To destroy CBI computer files, use software which completely overwrites the file.

CBI files no longer needed on the mainframe should be electronically overwritten by the user. CBI disks no longer needed must be returned to the DCO for information removal. In such cases, users must save whatever files they wish to retain, since ALL DISK ENTRIES WILL BE REMOVED.

## 3.8 USE IN NON-CBI DOCUMENTS

A coded or aggregate format must be used for the publication of study findings. CBI will not be identified in any publication or presentation by facility name or by variables, such as new technology or chemical use, which may reveal the facility identity.

## 3.9 INTERNAL AUDITS/VIOLATIONS

The DCO conducts announced and unannounced audits of EPA staff offices to check implementation of this Plan and/or to verify location of assigned documents. He reports findings to the branch chiefs and records security violations in a DCO Violations Log.

As determined to be necessary by the DCO, written reports on infractions are submitted to the responsible branch chief, requesting corrective action and written or verbal confirmation that action was taken.  A record of each such response is added to the Violations Log as verification of that action.  Upon repeat occurrence of the same or similar violations within two months after such notification, the DCO will report this finding to the branch chief and to the EAD Deputy Director.  More serious violations are reported immediately to the Deputy Director.

All employees who are authorized EAD CBI access are responsible for reporting to their DCO (1) possible violations, (2) the loss of CBI material, and/or (3) any unauthorized CBI disclosure.

## 4.0 TRANSMITTAL OF CBI

The EAD DCO will prepare, wrap and label all CBI material, including hard copy and disks, for transmittal outside of EPA Headquarters. Whenever possible, such transmittals should be sent to the DCO of the requester. All such material will be double-wrapped in a transmittal package or box, including a completed Transmittal Sheet (Figure 6). The originator sends this material to the DCO, along with a completed original and one copy of the Transmittal Sheet and a complete recipient address. The DCO retains the copy for temporary record and places the original inside the inner envelop, wrap or box before sealing and shipping. In addition, if copies have not previously been sent to recipients, the DCO will include one blank copy of the Transmittal Discrepancy Sheet (Figure 7). The requester uses this to report any problem with the material received.

The DCO may request or receive assistance in such preparation but must review each submission and initial the Transmittal Sheet before each package is sealed.

The Transmittal Sheet is not intended to be a transmittal memorandum with comments on analyses, policy or performance. The Transmittal Sheet only identifies the contents of the inner container in which it is sealed. The DCO prepares third party carrier forms and arranges pickup, if applicable. The EAD administrative staff arranges for annual renewals of such service agreements, with the DCO's approval.

Such material shall be kept inside two sealed, non-transparent (double-wrapped) covers. The inside cover will show the name and address of the recipient and both sides of that cover will be clearly stamped "CONFIDENTIAL BUSINESS INFORMATION", "TO BE OPENED BY ADDRESSEE ONLY." The outer cover will have the name and address of the recipient and sender -but no other markings indicating sensitivity of the contents. The outer wrap/cover may contain more than one internally wrapped document. The DCO maintains CBI cover sheets and materials to double wrap such material being sent outside of EAD.

When sending CBI to EPA contractors or to other EPA DCO's or staff, the sending DCO notifies the recipient when a shipment is ready, the number of boxes or envelops being sent, and the means of conveyance. Upon delivery, the recipient retains a copy of the Transmittal Sheet and notifies the DCO by phone or electronic mail within two hours of delivery. Within 24 hours, the recipient signs and sends a facsimile copy of the Transmittal Sheet to the DCO or mails the original. Any discrepancies will be explained by the recipient on the accompanying Transmittal Discrepancy Sheet.

The DCO transmits CBI to EPA and contractor staff and facilities through registered mail/return receipt requested. The DCO logs in the date and time each CBI item leaves his immediate control.

If short time transmittal is essential, CBI may also be sent using the U.S. Postal Service Express

Mail or a courier service such as Federal Express. CBI may be sent to a post office box number, as well as to an individual.

The DCO follows up with recipients outside of EAD through return receipts, phone calls or other appropriate means to confirm full and timely receipt of CBI material. In cases where such material is lost, damaged or delayed, the DCO will notify the requester. In the case of guaranteed delivery times by commercial carriers, delays will be reported to the EAD originator within 4 hours of scheduled delivery or as soon thereafter as the recipient replies. In case of delayed delivery, the DCO shall initiate tracing procedures with the carrier.

At no time will any CBI ever be sent over telephone facsimile/ modem lines (FAX), e-mail, or by regular U.S. Mail (rev. 1/27/99).

# GLOSSARY

Central CBI File

The physical repository of all CBI documents, except for hard drives on PCs, which are logged into EAD and are not -otherwise- signed out to staff.

Confidential
Business
Information

Is any disk or document received by EAD or by an EAD contractor, which is declared to be CBI by the submitting facility -or by a Project Manager in the case of CBI material generated within EAD or by a contractor.

Document

Normally a bound set of printed pages on a particular subject, but may include a single piece of paper; a computer disk; or a set of diskettes logged by the DCO as a single document, which are maintained together and which contain information about one project.

Facility

Any submitter of CBI from outside of EPA, including manufacturers, corporate offices, trade organizations, environmental organizations, law firms, consultants and individuals.

Locator Variables

Any indirect information which could identify a facility, especially when published in association with CBI derived analyses or information.

Project Officer

A contract manager in the Division, normally one for each EAD rule making project, who oversees the contractor's work, reviews and approves accomplishments and authorizes voucher claims for payment.

Project Manager

Refers to the staff person who is in charge of the development of a regulation. It does not refer to a contract "Project Officer," unless specifically so designated.

Master CBI Log

The log for initial entry, logging out and control of incoming CBI to the Division. Any other logs or CBI status reports are linked to and expand on information originally entered in this Log.

Working Folder

A CBI logged diskette or folder, which is handled as any other CBI document and contains CBI drafts, office generated reference material, and working papers that are not individually logged or use Cover Sheets.

Figure 1

## CONFIDENTIALITY AGREEMENT

I certify that I have read and fully understand the procedures outlined in the April 10, 2000 "Security Plan for Confidential Business Information in the Engineering and Analysis Division." I understand my responsibilities with respect to confidential business information (CBI) include:

- o using CBI only for the purpose of conducting EPA work
- o not disclosing the information to anyone other than authorized EPA staff or contractors
- o protecting CBI from loss while it is in my custody
- o returning all copies of CBI and any abstracts or excerpts therefrom to the Document Control Officer when no longer required, on completion of the project, or upon my termination or transfer from the Agency
- o agreement not to disclose any EAD CBI to any person after my termination or transfer from the Agency
- o complying with the required procedures presented in the April 10, 2000 Security Plan
- o promptly reporting to the Document Control Officer when this confidential access is no longer required.

____________________________
Signature (requesting person)

____________________________
Name (Printed)

____________________________
Office

____________________________
Date

____________________________
Telephone

____________________________      /    /
Document Control Officer      Date

Figure 2

**40 CFR § 2.301 and 2.302**

§2.301

(h) Disclosure to authorized representatives. (1) Under sections 114, 208 and 307(a) of the Act, EPA possesses authority to disclose to any authorized representative of the United States any information to which this section applies, notwithstanding the fact that the information might otherwise be entitled to confidential treatment under this subpart. Such authority may be exercised only in accordance with paragraph (h) (2) or (3) of this section.

(2)(i) A person under contract or subcontract to the United States government to perform work in support of EPA in connection with the Act or regulations which implement the Act may be considered an authorized representative of the United States for purposes of this paragraph (h). For purposes of this section, the term ``contract" includes grants and cooperative agreements under the Environmental Programs Assistance Act of 1984 (Pub. L. 98-313), and the term ``contractor" includes grantees and cooperators under the Environmental Programs Assistance Act of 1984. Subject to the limitations in this paragraph (h)(2), information to which this section applies may be disclosed:

(A) To a contractor or subcontractor with EPA, if the EPA program office managing the contract first determines in writing that such disclosure is necessary in order that the contractor or subcontractor may carry out the work required by the contract or subcontract; or

(B) To a contractor or subcontractor with an agency other than EPA, if the EPA program office which provides the information to that agency, contractor, or subcontractor first determines in writing, in consultation with the General Counsel, that such disclosure is necessary in order that the contractor or subcontractor may carry out the work required by the contract or subcontract.

(ii) No information shall be disclosed under this paragraph (h)(2), unless this contract or subcontract in question provides:

(A) That the contractor or subcontractor and the contractor's or subcontractor's employees shall use the information only for the purpose of carrying out the work required by the contract or subcontract, shall refrain from disclosing the information to anyone other than EPA without the prior written approval of each affected business or of an EPA legal office and shall return to EPA all copies of the information (and any abstracts or extracts therefrom) upon request by the EPA program office, whenever the information is no longer required by the contractor or subcontractor for the performance of the work required under the contract or subcontract, or upon completion of the contract or subcontract (where the information was provided to the contractor or subcontractor by an agency other than EPA, the contractor may disclose or return the information to that agency);

(B) That the contractor or subcontractor shall obtain a written agreement to honor such terms of the contract or subcontract from each of the contractor's or subcontractor's employees who will have access to the information, before such employee is allowed such access; and

(C) That the contractor or subcontractor acknowledges and agrees that the contract or subcontract provisions concerning the use and disclosure of business information are included for the benefit of, and shall be enforceable by, both the United States government and any affected business having an interest in information concerning it supplied to the contractor or subcontractor by the United States government under the contract or subcontract.

§2.302 **Special rules governing certain information obtained under the Clean Water Act.**

(2)-(3) The provisions of Sec. 2.301(h) (2) and (3) are incorporated by reference as paragraphs (h) (2) and (3), respectively, of this section.

# Excerpts from 40 CFR Para. 2.203, 2.209 and 2.211

**§2.203 Notice to be included in EPA requests, demands, and forms; method of asserting business confidentiality claim; effect of failure to assert claim at time of submission.**

(a) Notice to be included in certain requests and demands for information, and in certain forms. Whenever an EPA office makes a written request or demand that a business furnish information which, in the office's opinion, is likely to be regarded by the business as entitled to confidential treatment under this subpart, or whenever an EPA office prescribes a form for use by businesses in furnishing such information, the request, demand, or form shall include or enclose a notice which--

(1) States that the business may, if it desires, assert a business confidentiality claim covering part or all of the information, in the manner described by paragraph (b) of this section, and that information covered by such a claim will be disclosed by EPA only to the extent, and by means of the procedures, set forth in this subpart; (2) States that if no such claim accompanies the information when it is received by EPA, it may be made available to the public by EPA without further notice to the business; and

(3) Furnishes a citation of the location of this subpart in the Code of Federal Regulations and the Federal Register.

(b) Method and time of asserting business confidentiality claim. A business which is submitting information to EPA may assert a business confidentiality claim covering the information by placing on (or attaching to) the information, at the time it is submitted to EPA, a cover sheet, stamped or typed legend, or other suitable form of notice employing language such as trade secret, proprietary, or company confidential. Allegedly confidential portions of otherwise non-confidential documents should be clearly identified by the business, and may be submitted separately to facilitate identification and handling by EPA. If the business desires confidential treatment only until a certain date or until the occurrence of a certain event, the notice should so state.

**§2.209 Disclosure in special circumstances.**

(a) General. Information which, under this subpart, is not available to the public may nonetheless be disclosed to the persons, and in the circumstances, described by paragraphs (b) through (g) of this section. (This section shall not be construed to restrict the disclosure of information which has been determined to be available to the public. However, business information for which a claim of confidentiality has been asserted shall be treated as being entitled to confidential treatment until there has been a determination in accordance with the procedures of this subpart that the information is not entitled to confidential treatment.)

(b) Disclosure to Congress or the Comptroller General. (1) Upon receipt of a written request by the Speaker of the House, President of the Senate, chairman of a committee or subcommittee, or the Comptroller General, as appropriate, EPA will disclose business information to either House of Congress, to a committee or subcommittee of Congress, or to the Comptroller General, unless a statute forbids such disclosure.

(c) Disclosure to other Federal agencies. EPA may disclose business information to another Federal agency if--

(1) EPA receives a written request for disclosures of the information from a duly authorized officer or employee of the other agency or on the initiative of EPA when such disclosure is necessary to enable the other agency to carry out a function on behalf of EPA;

(d) Court-ordered disclosure. EPA may disclose any business information in any manner and to the extent ordered by a Federal court. Where possible, and when not in violation of a specific directive from the court, the EPA office disclosing information claimed as confidential or determined to be confidential shall provide as much advance notice as possible to each affected business of the type of information to be disclosed and to whom it is to be disclosed, unless the affected business has actual notice of the court order. At the discretion of the office, subject to any restrictions by the court, such notice may be given by notice in the Federal Register, letter sent by certified mail return receipt requested, or telegram.

(e) Disclosure within EPA. An EPA office, officer, or employee may disclose any business information to another EPA office, officer, or employee with an official need for the information.

(f) Disclosure with consent of business. EPA may disclose any business information to any person if EPA has obtained the prior consent of each affected business to such disclosure.

(g) Record of disclosures to be maintained. Each EPA office which discloses information to Congress, a committee or subcommittee of Congress, the Comptroller General, or another Federal agency under the authority of paragraph (b) or (c) of this section, shall maintain a record of the fact of such disclosure for a period of not less than 36 months after such disclosure. Such a record, which may be in the form of a log, shall show the name of the affected businesses, the date of disclosure, the person or body to whom disclosure was made, and a description of the information disclosed.

Sec. 2.211 Safeguarding of business information; penalty for wrongful disclosure.

(a) No EPA officer or employee may disclose, or use for his or her private gain or advantage, any business information which came into his or her possession, or to which he or she gained access, by virtue of his or her official position or employment, except as authorized by this subpart.

(b) Each EPA officer or employee who has custody or possession of business information shall take appropriate measures to properly safeguard such information and to protect against its improper disclosure.

(c) Violation of paragraph (a) or (b) of this section shall constitute grounds for dismissal, suspension, fine, or other adverse personnel action. Willful violation of paragraph (a) of this section may result in criminal prosecution under 18 U.S.C. 1905 or other applicable statute.

(d) Each contractor or subcontractor with the United States Government, and each employee of such contractor or subcontractor, who is furnished business information by EPA under Secs. 2.301(h), Sec. 2.302(h), 2.304(h), 2.305(h), 2.306(j), 2.307(h), 2.308(i), or 2.310(h) shall use or disclose that information only as permitted by the contract or subcontract under which the information was furnished. Contractors or subcontractors shall take steps to properly safeguard business information including following any security procedures for handling and safeguarding business information which are contained in any manuals, procedures, regulations, or guidelines provided by EPA. Any violation of this paragraph shall constitute grounds for suspension or debarment of the contractor or subcontractor in question. A willful violation of this paragraph may result in criminal prosecution.

Figure 3

Date

MEMORANDUM

SUBJECT: Request Access to OST Confidential Business Information

FROM: (Your name, Office mail code and phone number)

TO: David Hoadley, Document Control Officer  
Engineering and Analysis Division, OST 4303

THRU: 1. EAD Branch Chief (knowledgeable about your requirement)  
2. Sheila Frace, Director *  
Engineering and Analysis Division

I request authorization for access to the confidential business information controlled by the Engineering and Analysis Division to ________________________________(state specific reason)________________________________. This work is required by my EPA position as a ____(position title)________ in the ________(organization title)__________, which is currently working on ______(general requirement or context for the reason above)______________________________________. I will require access to this information for approximately ______(number of weeks/months)_______.

I acknowledge that this authorization will not exceed one year. If my requirement for this CBI ends at an earlier time than stated above, I will notify the Document Control Officer (DCO) to that effect and return any EAD CBI to the DCO.

I have read and understand the "Security Plan for Confidential Business Information in the Engineering and Analysis Division," as amended April 10, 2000 along with the attached provisions of 40 CFR Part 2 and agree to comply with it. I have the necessary double locked security in my office as specified in the "Plan" to safeguard any CBI material signed out to me. I understand that my last requirement for CBI clearance, after your approval, will be to pass the written test for the Plan, to sign the "Confidentiality Agreement" and give that original signed statement to the DCO, along with the original of this approved memorandum.

Approve __ Disapprove __

________________________________

* Sheila Frace, Director  
Engineering and Analysis Division

Figure 4

DO NOT DETACH

# CONFIDENTIAL BUSINESS INFORMATION

| | | |
|---|---|---|
| DOCUMENT CONTROL OFFICER | DOCUMENT IDENTIFICATION NO. | DATE RECEIVED |

**The attached document contains Confidential Business Information obtained under the Clean Water Act (CWA).**

**If you willfully disclose CWA Confidential Business Information to any person not authorized to receive it you may be liable under 18 U.S.C. 1905 for a possible fine up to $1,000 and/or imprisonment for up to one year. In addition, disclosure of CWA Confidential Business Information or violation of the procedures cited above may subject you to disciplinary action with penalties ranging up to and including dismissal.**

**Each person who is given access to this document must fill in the information below.**

| NAME OF USER/OFFICE (Please print) | USER'S (Printed) | NAME (Signed) | DATE OUT | DATE TO CENTRAL CBI FILE | DCO INITIAL |
|---|---|---|---|---|---|
| | | | | XXXX | |
| XXXXXXXX | XXXXXXXXXX | XXXXXXX | XXX | | |

* * * IF A NON-CBI CLEARED PERSON ENTERS YOUR OFFICE, * * *
THIS DOCUMENT MUST BE PLACED FACE DOWN, COVERED OR FILED

* * * WHEN LEAVING YOUR OFFICE FOR A SHORT TIME, * * *
THIS DOCUMENT MUST BE IN A LOCKED FILE CABINET OR DESK

* * * WHEN LEAVING THE OFFICE FOR A LENGTHY PERIOD * * *
OR AT THE END OF THE DAY,
THIS DOCUMENT MUST BE PLACED BEHIND TWO LEVELS OF LOCKS

* * * THIS DOCUMENT MUST BE HAND DELIVERED, * * *
WHEN IT MOVES BETWEEN OST OFFICES

* * * IF THIS DOCUMENT IS FOUND UNATTENDED, * * *
IT MUST BE RETURNED TO THE DCO

* * * ONLY THE EAD DCO IS AUTHORIZED * * *
TO MAKE A COMPLETE COPY OF THIS DOCUMENT,
EXCEPT FOR A DOCUMENT CREATED WITHIN EAD
- WHICH MAY BE COPIED BY THE ORIGINATOR

Figure 5

SIGN-OUT SHEET
for
CONFIDENTIAL BUSINESS INFORMATION

* * * * * * * * * * MAINTAIN VISIBLY IN EACH OFFICE * * * * * * * * * *

- - - DOCUMENTS SHALL NOT BE LOANED FOR MORE THAN ONE WEEK - - -

The Borrower acknowledges responsibility for safeguarding the Confidential Business Information (CBI) material received, until returned to the "Original User." The latter is that individual who originally received this material from the DCO. All borrowed CBI will be returned to the Original User.

| | BORROWER | | ORIGINAL USER | |
|---|---|---|---|---|
| Document ID # | Date Signed Out to . . | Signature Loaned to | Date Returned | Signature of Recipient |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Figure 6

# TRANSMITTAL SHEET

DATE SHIPPED:___/___/___ BOX #:_____ PAGE ___ OF___

TO:______________________________
*Name and organization*

FROM:____________________________
*Name and organization*

METHOD OF DELIVERY:______________

| SURVEY ID OR DCN | DESCRIPTION | CBI Y/N | RECEIPT VERIFIED (INITIALS) |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

*<u>INSTRUCTIONS</u>*

1. *The sender will notify the recipient when a shipment is ready and give the number of boxes in the shipment.*
2. *This transmittal sheet is to be sealed inside each box before the box is shipped.*
3. *A copy of the transmittal sheet is to be retained by the sender.*
4. *Original of this transmittal sheet is to be signed by the recipient and returned to the sender.*
5. *Duplicate of the signed transmittal sheet is to be retained by the recipient.*
6. *Any discrepancies are to be explained on the "Transmittal Discrepancy Sheet."*

________________________________________________________
Recipient's signature Date Received

Figure 7

# TRANSMITTAL DISCREPANCY SHEET

(Please record discrepancies for each transmittal on a separate sheet.)

## TO BE COMPLETED BY RECEIVER:

Contact person:______________________________ phone #:(_____)______________

Transmittal Information

Date of transmittal:__________

Origin of transmittal:__________________________________________________
Individual's name and organization

Destination of transmittal:_____________________________________________
Individual's name and organization

Mode of delivery:_______________________

Date transmitter notified by phone of discrepancy:___________

Identification of Discrepancy:

*(if more space is necessary, attach a page listing the items below)*

| Box # | Survey id/DCN | Problem |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## TO BE COMPLETED BY TRANSMITTER:

Resolutions:

____________________________________________________________

____________________________________________________________

____________________________________________________________

Signature:_________________________________ Date:_________

Resolution approved by________________________
*Branch Chief or Supervisor*

Instructions:
Return copies of completed form to receiver and to the OST DCO.

Figure 8

Office of Science and Technology
DESTRUCTION LOG

DCO/ADCO NAME ____________________________ LOCATION ________________

| DATE<br>DESTROYED | DOCUMENT<br>ID # | DESTRUCTION | DCO/ADCO<br>SIGNATURE |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Figure 9 (For those cleared under other EPA CBI plans)

Date

MEMORANDUM

SUBJECT: Request Access to EAD, OST
Confidential Business Information

FROM: (Your name, office mail code and phone number)

TO: David Hoadley, Document Control Officer
Engineering and Analysis Division, OST 4303

THRU: 1. EAD Project Officer (knowledgeable about your requirement)
2. Sheila Frace, Director*
Engineering and Analysis Division

I request authorization for access to the confidential business information controlled by the Engineering and Analysis Division to ______________________________(state specific reason)__________. This work is required by my EPA position as a ___(position title)____ in the ______(organization title)_____. This office is currently working on ______(general mission requirement of your office)__________. I will require access to this information for approximately (number of months).

I acknowledge that this authorization, which may be renewed, will not exceed one year. If my requirement for this CBI ends earlier than stated above, I will notify the EAD Document Control Officer (DCO) to that effect and return any EAD CBI to him.

I have read and understand the "Security Plan for Confidential Business Information in the Engineering and Analysis Division, as amended April 10, 2000," and agree to comply with it, while requested CBI is under the control of that Division. I understand that the original of this memorandum, when approved by you, must be received by your DCO before my clearance becomes effective.

Cleared under (program name) CBI Plan

Signature________________________
(Name and phone number of your
program's CBI officer)

Approve ____ Disapprove ____

______________________________________
* Sheila Frace, Director
Engineering and Analysis Division

## Appendix B

# OST-CBI Application Rules of Behavior

OST's Engineering & Analysis Division (EAD) relies on the OST-CBI application and its data to support the effluent guidelines program and other programs. Therefore, everyone using the OST-CBI application is responsible for complying with the rules and procedures in this section.

**All OST-CBI application users must protect the application and its data from loss, misuse, and unauthorized access or modification.**

Failure to follow the rules listed in this section may result in one or more of the following actions:

- Suspension of access privileges
- Reprimand
- Suspension or Removal

Note: *If you do not comply, the consequences will be based on the severity of the violation (at management's discretion), and through due process of law.*

### Important Phone Numbers

| | |
|---|---|
| ***Application Security Manager (ASM)***<br>Gregory Stapleton | (202) 566-1028 |
| ***Document Control Officer (DCO)***<br>George Jett | (202) 566-1070 |
| ***RACF Security Administrator (RSA)***<br>Jade Lee-Freeman | (202) 566-1074 |
| ***Alternate RSA***<br>Leonid Kopylev | (202) 566-2237 |
| ***LAN Manager***<br>Vera Williams-Bower | (202) 566-0412 |
| ***OW's Information Security Officer (ISO)***<br>Terry Howard | (202) 564-0385 |
| ***National Computer Center (NCC) Help Desk*** | (800) 334-2405 |

## EPA and Contractor Staff Rules

- ***Acquire and maintain up-to-date certifications for the following*:**
  - **Information Technology (IT) Security Awareness E-Learning Training Program.** OEI provides this training through the EPA intranet. Certification must be renewed annually.
  - **CBI Security Training.** The DCO provides this training on an as-needed basis. Certification must be renewed biannually for EAD staff and annually for others. Certification requires signing a Confidentiality Agreement. See *Security Plan for Confidential Business Information in the Engineering and Analysis Division*.

  The ASM maintains a list of personnel possessing the above certifications.

- ***Protect the OST-CBI application and data from unauthorized disclosure and loss of integrity.*** The *Security Plan for Confidential Business Information in the Engineering and Analysis Division* describes safeguards to protect CBI regarding several situations, including:
  - office use
  - telephone conversations
  - meetings
  - printing
  - home use
  - transmittal
  - reproduction

- ***Do not transmit CBI through unauthorized means, such as:***
  - *E-mail*
  - *Inter-office mail.*

  For correct transmittal procedures, see *Security Plan for Confidential Business Information in the Engineering and Analysis Division*.

- ***Do not store CBI on hard drives or LAN drives.***
- ***Do not run or obtain data from the OST-CBI application for unauthorized individuals.*** The ASM, DCO, or RSA can verify whether the individual is authorized to use the OST-CBI application.
- ***Notify the RSA when you are not going to use mainframe OST-CBI for 3 months or more.***
- ***Notify the ASM, DCO, or RSA of security incidents immediately*.**

| | |
|---|---|
| ***Application Security Manager (ASM)***<br>Gregory Stapleton | (202) 566-1028 |
| ***Document Control Officer (DCO) - Acting***<br>George Jett | (202) 566-1070 |
| ***RACF Security Administrator (RSA)***<br>Jade Lee-Freeman | (202) 566-1074 |

Security incidents **include** instances where you observe the following:

- Inappropriate transmission of CBI
- Disclosure of CBI to unauthorized personnel
- Unattended or inappropriately stored CBI
- Violations of the *Security Plan for Confidential Business Information in the Engineering and Analysis Division*

- ***Protect your passwords, including those you use for the mainframe, LAN, and Lotus Notes .***
    - *Do not use someone else's passwords.*
    - *Use different passwords for the EPA LAN and the mainframe.*
    - *Memorize your passwords - don't write them down.*
    - *Never put your password into a login script.*
- ***Control access to your PC***
    - *Use a screen saver with a password on your PC.* Set it to display after 5 minutes of no activity or less.
    - *Logout and turn-off your PC when you leave work for the day.*
- ***Do not attempt to view, change, or delete data, unless you are authorized.***

**Note: The ASM, DCO, or RSA, may perform "spot checks" to verify that you are complying with these rules.**

### EPA Supervisor, Project Manager, and Task Leader Rules

- ***Follow the rules of behavior for EPA and contractor staff.***
- ***Review access requests for the OST-CBI application.*** *Requests must include the following:*

  1. *what the employee needs to access,*
  2. *the access privileges desired, and*
  3. *adequate justification for the above.*

  If you agree with the request, forward it to the DCO (paper and removable media OST-CBI) or the RSA (mainframe CBI).

- ***If you are a supervisor, notify the ASM when one of your staff is going to transfer, resign, or be terminated.*** You must keep appropriate records to document you have met this requirement.

## EPA Project Officers

- ***Follow the rules of behavior for EPA and contractor staff.***
- ***Ensure that a contractor under an EAD contract adopts a CBI security plan compatible with the*** **Security Plan for Confidential Business Information in the Engineering and Analysis Division,** ***as described in Section 2.3 of that plan.*** You must consult with the DCO, RSA, and ASM before you approve a contractor's CBI security plan.
- ***Require contractor staff, through appropriate contract language, to acquire and maintain the following certifications if they need access to the OST-CBI application:***
  - **Information Technology (IT) Security Awareness E-Learning Training Program.** OEI provides this training through the EPA intranet. Certification must be renewed annually.
  - **CBI Security Training.** Certification requires signing a Confidentiality Agreement. The document control officer (DCO) or ASM provides this training on an as-needed basis. Certification must be renewed annually. See *Security Plan for Confidential Business Information in the Engineering and Analysis Division*.
- ***Provide the DCO, RSA, and ASM (on a monthly basis) a list of authorized mainframe users under your contracts.*** Please specify the following on this list:
  - which contractor users will be absent for a month or more,
  - which contractor users no longer need to use mainframe OST-CBI application under your contract, and
  - which contractor users no longer need to use paper and removable media OST-CBI application under your contract.

**Note: You must keep appropriate records to show you've met the above requirements.**

## WAM Rules

- ***Follow the rules of behavior for EPA and contractor staff.***
- ***Request access for contractor staff under your work assignment if they need to use the OST-CBI application.*** Employee requests must include the following:

  1. what the contractor needs to access,
  2. the desired access privileges, and
  3. adequate justification for the above.

  Send the completed request to the appropriate project manager, task leader, or your immediate supervisor.

**Document Control Officer (DCO)**

- ***Follow the rules of behavior for EPA and contractor staff.***
- ***Before you grant access to paper and removable media CBI to EPA staff, they must e-mail you a request that states 1) what they need to access , 2) the access privileges they desire, and 3) adequate justification for both.***
    - The appropriate project manager, task leader, or their immediate supervisor must agree with this request.
    - The potential user must be certified as having successfully completed the training described above under **EPA and Contractor Staff Rules**.

  If you are satisfied the requirements have been fulfilled, grant access only to the CBI documents that permits the user to do their job.
- ***Before granting access to paper and removable media CBI to contractor staff, their WAM must e-mail you a request that states 1) what they need to access , 2) the access privileges they desire, and 3) adequate justification for both.***
    - Their project manager, task leader, or immediate supervisor of must agree with this request.
    - The potential user must have successfully completed the training described above under **EPA and Contractor Staff Rules**.

  If you are satisfied the requirements have been fulfilled, grant access only to the CBI documents that permits the user to do their job.
- ***Deny access a paper and removable media CBI user when one or more of the following conditions exist:***
    - *The user's supervisor has informed you that a user is going to be transferred, resign, or be terminated.* The supervisor will provide the effective date.
    - *One or more certifications for the user have expired.*

    You may remove a user's access during other circumstances, provided you have appropriate justification.
- ***Before a user's access expires or is terminated, retrieve any paper and removable media CBI from the user.***
- ***Track paper and removable media CBI (original and paper) as described under the*** **Security Plan for Confidential Business Information in the Engineering and Analysis Division.**
- ***Notify the appropriate personnel of security policy violations immediately.***
- ***Conduct activities to promote the security of the OST-CBI application.***

**Note: You must keep appropriate records to show you've met the above requirements.**

### RACF Security Administrator (RSA) Rules

- ***Follow the rules of behavior for EPA and contractor staff.***
- ***You must receive and maintain RACF certification.*** You must renew your certification biannually. RTP mainframe instructors routinely provide training. You may be required to update your certification more frequently based on changes to the mainframe system or RACF responsibilities.
- ***Before you grant access to mainframe OST-CBI to EPA staff, they must e-mail you a request that states 1) what they need to access, 2) the access privileges they desire, and 3) adequate justification for both.***
  - Their project manager, task leader, or immediate supervisor of must agree with this request.
  - The potential user must have successfully completed the training descibed above under **EPA and Contractor Staff Rules**.

  If you are satisified the requirements have been fulfilled, grant the lowest access level that still permits the user to do their job.
- ***Before granting access to mainframe OST-CBI to contractor staff, the WAM must e-mail you a request that states 1) what they need to access , 2) the access privileges they desire, and 3) adequate justification for both.***
  - Their project manager, task leader, or immediate supervisor of must agree with this request.
  - The potential user must have successfully completed the training descibed above under **EPA and Contractor Staff Rules**.

  If you are satisified the requirements have been fulfilled, grant the lowest access level that still permits the user to do their job.
- ***Remove access from a mainframe OST-CBI user when one or more of the following conditions exist:***
  - *The user's supervisor has informed you that he or she is going to be transferred, resign, or be terminated.* The supervisor will provide the effective date.
  - *The user's account has not been used for 3 months.*
  - *One or more certifications for the user have expired.*

  You may remove a user's access during other circumstances, provided you have appropriate justification.
- ***Notify the appropriate personnel of security policy violations immediately.***
- ***Conduct activities to promote the security of the OST-CBI application.***

**Note: You must keep appropriate records to show you've met the above requirements.**

### Application Security Manager Rules

- ***Follow the rules of behavior for EPA and contractor staff.***
- ***Maintain a list of EPA and contractor personnel authorized to access the OST-CBI application and its data.*** Authorized personnel possess the following certifications:
  - Information Technology (IT) Security Awareness E-Learning Training Program
  - CBI Security Training.
- ***Recommend and apply security mechanisms to protect the OST-CBI application.***
- ***Conduct periodic security reviews to verify that users, DCOs and RSAs are complying with their rules of behavior.***
- ***On a monthly basis at a minimum, discuss the status of the OST-CBI application and related issues with the NTSD representative identified in Section 1.4 of the OST-CBI major application security plan.*** Informal e-mails or other methods may be used to document these discussions.
- ***Provide appropriate training to EPA, contractor, and other personnel who use or support the OST-CBI application.*** You must document that they have received this training.
- ***Notify the appropriate personnel of security policy violations immediately.***
- ***Conduct activities to promote the security of the OST-CBI application.***

**Note: You must keep appropriate records to show you've met the above requirements.**